

11/09/99



jc490 U.S. PRO

UTILITY PATENT APPLICATION TRANSMITTAL

Submit an original and a duplicate for fee processing
(Only for new nonprovisional applications under 37 CFR §1.53(b))

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

Attorney Docket No. 200310
First Named Inventor VAN GUNTER
Express Mail No. EM196184425US

jc625 U.S. PRO

09/436135



11/09/99

APPLICATION ELEMENTS

1. ☒ Utility Transmittal Form
2. ☒ Specification (including claims and abstract) [Total Pages 25]
3. ☒ Drawings [Total Sheets 5]
4. ☒ Combined Declaration and Power of Attorney [Total Pages 3]
 - a. ☒ Newly executed
 - b. ☐ Copy from prior application
[Note Box 5 below]
 - i. ☐ Deletion of Inventor(s) Signed statement attached deleting inventor(s) named in the prior application
5. ☐ Incorporation by Reference: The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Microfiche Computer Program
7. ☐ Nucleotide and/or Amino Acid Sequence Submission
 - a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy
 - c. ☐ Statement verifying above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet and document(s))
9. ☐ Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement (IDS)
 - ☐ Form PTO-1449
 - ☐ Copies of References
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (Should be specifically itemized)
14. ☐ Small Entity Statement(s)
 - ☐ Enclosed
 - ☐ Statement filed in prior application; status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
16. ☒ Other: A check in the amount of \$800.00

17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information in (a) and (b) below:
- (a) ☐ Continuation ☐ Divisional ☐ Continuation-in-part of prior application Serial No. .
Prior application information: Examiner ; Group Art Unit:
- (b) Preliminary Amendment: Relate Back - 35 USC §120. The Commissioner is requested to amend the specification by inserting the following sentence before the first line:
"This is a ☐ continuation ☐ divisional of copending application(s)
☐ Serial No. , filed on .
☐ International Application, filed on , and which designates the U.S."

APPLICATION FEES

BASIC FEE				\$760.00
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total Claims	15 -20=	0	x \$18.00	\$0.00
Independent Claims	2 - 3=	0	x \$78.00	\$0.00
<input type="checkbox"/> Multiple Dependent Claims(s) if applicable			+\$260.00	\$
Total of above calculations =				\$
Reduction by 50% for filing by small entity =				\$()
<input checked="" type="checkbox"/> Assignment fee if applicable			+ \$40.00	\$40.00
TOTAL =				\$800.00

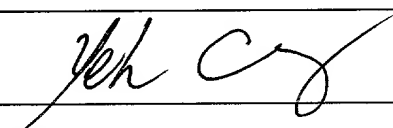
UTILITY PATENT APPLICATION TRANSMITTAL

Attorney Docket No. 200352

19. ☐ Please charge my Deposit Account No. 12-1216 in the amount of \$.
20. ☒ A check in the amount of \$800.00 is enclosed.
21. The Commissioner is hereby authorized to credit overpayments or charge any additional fees of the following types to Deposit Account No. 12-1216:
- a. ☒ Fees required under 37 CFR §1.16.
- b. ☒ Fees required under 37 CFR §1.17.
22. ☒ The Commissioner is hereby generally authorized under 37 CFR §1.136(a)(3) to treat any future reply in this or any related application filed pursuant to 37 CFR §1.53 requiring an extension of time as incorporating a request therefor, and the Commissioner is hereby specifically authorized to charge Deposit Account No. 12-1216 for any fee that may be due in connection with such a request for an extension of time.

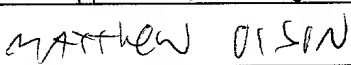
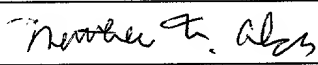
23. CORRESPONDENCE ADDRESS

Y. Kurt Chang, Registration No. 41,397
Leydig, Voit & Mayer, Ltd.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
Telephone: (312) 616-5600
Facsimile: (312) 616-5700

Name	Y. Kurt Chang, Reg. No. 41,397
Signature	
Date	November 9, 1999

Certificate of Mailing Under 37 CFR §1.10

I hereby certify that this Utility Patent Application Transmittal and all accompanying documents are being deposited with the United States Postal Service "Express Mail Post Office To Addressee" Service under 37 CFR §1.10 on the date indicated below and is addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231.

		November 9, 1999
Name of Person Signing	Signature	Date

SYSTEM AND METHOD OF USER AUTHENTICATION FOR NETWORK
COMMUNICATION THROUGH A POLICY AGENT

5

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to network communication and, more particularly, to the communication between a computer on a first network with another computer on a second network through a policy agent of the first network.

10

BACKGROUND OF THE INVENTION

Computers in an organization are often linked together to form a private network so that the computers can communicate with each other and share resources. Such an internal computer network within the control of an organization is commonly referred to as an "intranet." Many intranets are composed of local area networks, although the intranets of some large organizations have grown very large and require the level of sophistication found in the Internet.

15

Today's network environment demands secure data communications. A major concern for private networks is the possibility of security breach through communications with external networks. As the Internet and the World Wide Web become the essential backbone for worldwide commerce and information sharing, the need for manageable and secure networks becomes more urgent than ever. A fundamental key to the implementation of a secure network is the ability to manage network access. To protect the integrity and vital data of an intranet, a network administrator has to be able to

20

25

004335 11099
"SECRET"

implement policies to restrict access to certain users or sources. The restrictions may be based on various parameters, such as user credentials, the source address, the destination address, time of the day, etc. To that end, a policy agent
5 standing between a private network and an external network, such as the Internet, is typically the focal point for carrying out the network access policies. A policy agent may be, for example, a network firewall that guards the intranet and hides its structure from the outside by filtering
10 communication packets or performing session-based application-level access control.

A successful implementation of access control often requires the capability of applying access policies based on user credentials, i.e., who the user is, whom the user is
15 allowed to send or receive network communication to or from, etc. The commonly used network protocols, however, typically do not lend themselves to user authentication in connection with network access. Network communication data are represented in a variety of network protocols. Each of the
20 existing network protocols serves one or more technical purposes within a network environment. Typically, under those protocols, only the source and destination addresses and ports are provided in the header of the network data, and the access policies are typically limited to those parameters. The lack
25 of user information in the communication packets makes it very difficult to implement network policies based on user credentials. It is possible, of course, to create a new

SECRET 3213460

network protocol that includes information for user authentication in the data stream. Such a solution, however, may not be preferred, as it will require almost all existing network applications to be rewritten to accommodate the new
5 protocol.

SUMMARY OF THE INVENTION

In view of the foregoing, the present invention provides a method and system for a policy agent of a network to
10 authenticate a user that uses a client computer on the network to transmit network communication data, and to associate the data stream from the client computer with the user. When the client computer initiates a network data connection to or through the policy agent, the policy agent detects the data
15 connection and sends a challenge to the client computer. The challenge is encrypted with a private key of the policy agent. When the client computer received the challenge, it decrypts the challenge with the public key of the policy agent and prepares a message digest value, such as by a hash algorithm,
20 based on the data in the challenge and the network data sent by the user. The message digest value is then encrypted with the private key of the user and sent to the policy agent. The policy agent decrypts the received response with the public key of the user to obtain the message digest value. The
25 policy agent then calculates a digest value based on the challenge and the network data received from the client computer, and compares the calculated digest value with the

665011-5E9E460

digest value decrypted from the response. If the two digest values match, the policy agent knows that the user has been authenticated, and that the received network data are those sent by the user. The policy agent may then apply network
5 policies based on the credentials of the authenticated user.

Additional features and advantages of the invention will be made apparent from the following detailed description of illustrative embodiments which proceeds with reference to the accompanying figures.

10

BRIEF DESCRIPTION OF THE DRAWINGS

While the appended claims set forth the features of the present invention with particularity, the invention, together with its objects and advantages, may be best understood from
15 the following detailed description taken in conjunction with the accompanying drawings of which:

Figure 1 is a block diagram generally illustrating an exemplary computer system on which the present invention resides;

20 FIG. 2 is a schematic diagram showing a client computer on a network transmitting network data through a policy agent of the network;

FIG. 3 is a schematic diagram illustrating communications
25 between the policy agent and the client computer for a user authentication process;

656077 SEF9460

FIG. 4 is a flow chart showing an embodiment of the user authentication process for network data transmitted through the policy agent;

FIG. 5 is a schematic diagram illustrating the generation of a challenge sent by the policy agent to the client computer for user authentication;

FIG. 6 is a schematic diagram illustrating the generation of a response by the client computer; and

FIG. 7 is a schematic diagram illustrating the use of the response for authenticating the user and associating the received network data to the user.

DETAILED DESCRIPTION OF THE INVENTION

Turning to the drawings, wherein like reference numerals refer to like elements, the invention is illustrated as being implemented in a suitable computing environment. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like.

The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be
5 located in both local and remote memory storage devices.

With reference to Fig. 1, an exemplary system for implementing the invention includes a general purpose computing device in the form of a conventional personal computer 20, including a processing unit 21, a system memory
10 22, and a system bus 23 that couples various system components including the system memory to the processing unit 21. The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures.
15 The system memory includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system (BIOS) 26, containing the basic routines that help to transfer information between elements within the personal computer 20, such as during start-up, is stored in ROM 24. The personal
20 computer 20 further includes a hard disk drive 27 for reading from and writing to a hard disk 60, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to a removable optical disk 31 such as a CD ROM or other optical
25 media.

The hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a

66601T" GET 92450

hard disk drive interface 32, a magnetic disk drive interface 33, and an optical disk drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for the personal computer 20. Although the exemplary environment described herein employs a hard disk 60, a removable magnetic disk 29, and a removable optical disk 31, it will be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories, read only memories, and the like may also be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk 60, magnetic disk 29, optical disk 31, ROM 24 or RAM 25, including an operating system 35, one or more applications programs 36, other program modules 37, and program data 38. A user may enter commands and information into the personal computer 20 through input devices such as a keyboard 40 and a pointing device 42. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port or a universal serial bus (USB). A monitor 47 or other

type of display device is also connected to the system bus 23 via an interface, such as a video adapter 48. In addition to the monitor, personal computers typically include other peripheral output devices, not shown, such as speakers and
5 printers.

The personal computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 49. The remote computer 49 may be another personal computer, a server, a router, a
10 network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the personal computer 20, although only a memory storage device 50 has been illustrated in Fig. 1. The logical connections depicted in Fig. 1 include a local area network
15 (LAN) 51 and a wide area network (WAN) 52. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the personal computer 20 is connected to the local network 51 through a
20 network interface or adapter 53. When used in a WAN networking environment, the person computer 20 typically includes a modem 54 or other means for establishing communications over the WAN 52. The modem 54, which may be internal or external, is connected to the system bus 23 via
25 the serial port interface 46. In a networked environment, program modules depicted relative to the personal computer 20, or portions thereof, may be stored in the remote memory

storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

5 In the description that follows, the invention will be described with reference to acts and symbolic representations of operations that are performed by one or more computers, unless indicated otherwise. As such, it will be understood that such acts and operations, which are at times referred to
10 as being computer-executed, include the manipulation by the processing unit of the computer of electrical signals representing data in a structured form. This manipulation transforms the data or maintains it at locations in the memory system of the computer, which reconfigures or otherwise alters
15 the operation of the computer in a manner well understood by those skilled in the art. The data structures where data is maintained are physical locations of the memory that have particular properties defined by the format of the data. However, while the invention is being described in the
20 foregoing context, it is not meant to be limiting as those of skill in the art will appreciate that various of the acts and operation described hereinafter may also be implemented in hardware.

Referring now to FIG. 2, the present invention is
25 directed to a system and method of authenticating a user 70 that uses a client computer 72 on a network 74 to send a network data stream 76 through a policy agent 78 of the

665011-GET-9E460

network. As shown in FIG. 2, the policy agent 78 is the connection point, or gateway, between the network 74 of the client computer and another network 80 on which the recipient computer 82 resides. The policy agent may be, for example, a network firewall. In a preferred embodiment, the first network 74 on which the client computer 72 resides is an intranet, and the second network 80 is an external network, such as the Internet. When the user 70 uses the client computer 72 to send network data to the recipient computer 82 on the external network, the network data is directed to the policy agent 78, which applies access policies to determine whether to pass the network data to or from the recipient computer.

In accordance with a feature of the invention, the policy agent 78 carries out a user-authentication process that authenticates the user 70 who sends the network data 76 and associates the network data received from the client computer with the authenticated user. In other words, the policy agent 78 verifies that user 70 is indeed who she claims to be, and verifies that the received network data are indeed those sent by that user. The user authentication enables the policy agent to apply access policies based on the credentials of the user. As will be described in greater detail below, the user authentication according to the invention is secure from malicious alterations, such as by a man-in-the-middle attack, user credential spoofing, or a reply attack.

Moreover, the authentication process is independent of the particular network protocol used for transmitting the network data. In accordance with a feature of the invention, the user authentication is performed out-of-band, i.e., the network communications for the authentication process are not part of network data stream on which the network policies are to be applied. Few network protocols commonly used for network data transmission have provisions for inclusion of user authentication information as part of the data stream.

If an in-band user authentication is to be implemented, those network protocols would have to be substantially modified or entirely replaced with new protocols. Such a solution, however, may not be practical or desirable. The out-of-band user authentication in accordance with the invention avoids the need to include user authentication information in the network data stream on which access policies are to be applied. As a result, the authentication process is independent of the underlying network protocol used to send the data stream and can be used with existing network protocols. With out-of-band user authentication, however, there is a risk that the user information may be altered or incorrectly associated with the network data stream. As will be described in greater detail below, the user authentication according to the invention effectively avoids this risk by including data from the network data stream in the digital signature process used in the user authentication.

Turning now to FIG. 3, the user authentication process includes the sending of a challenge 90 by the policy agent 78 to the client computer 72 that initiated the network connection 92, and the returning of a response 94 by the client computer to the policy agent. This challenge-response sequence employs a public key/private key encryption scheme for authenticating the identity of the user. The response 94 also includes information regarding the network data to enable the policy agent to confirm that the received network data are those sent by the user. In a preferred embodiment, the network data are in the form of data packets 96.

An embodiment of the authentication process is illustrated in FIG. 4. When the client computer located on the network initiates a network data connection either to or through the policy agent (step 100), the out-of-band authentication process is initiated. When the policy agent detects the new network connection (step 102), it obtains the purported identity of the user (step 104). Various ways can be used to obtain the identity of the user associated with the network connection with the client computer. For example, in a preferred embodiment, the source information in the network data may include the address and port number of the client computer that sent the data. A query may be sent to a directory service 84 (FIG. 2) that keeps track of the current configuration and usage of the computers on the network. In response, the directory service 84 returns the identity of the user currently at the source address and port number. It will

be appreciated that the invention is not limited to any specific mechanism used for obtaining the identity of the unauthenticated user associated with the network connection.

After the policy agent has obtained the purported
5 identity of the user associated with the network connection, it obtains a public key of the user (step 106). This may be done, for example, by querying a registry 86 (FIG. 1) that maintains a file of public keys of users registered with it. The registry 86 may be separate or the same as the directory
10 server 84. The policy agent then constructs a challenge 90 that is encrypted with its own private key (step 108). The challenge 90 is sent to the client computer 72 (step 110).

When the client computer 72 receives the challenge 90, it decrypts the challenge using the policy agent's public key
15 (step 112). The client computer then generates a first message digest value based on the data from the decrypted challenge and the network data transmitted to the policy agent (STEP 114). The first message digest value is encrypted with the private key of the user to form a response to the
20 challenge (step 116), and the response is sent to the policy agent (step 118). When the policy agent receives the response, it decrypts the response with the public key of the user to obtain the first message digest value (step 120). It then calculates a second message digest value from the
25 challenge and the network data it received from the client computer (step 122). The policy agent then compares the digest value it calculated with the digest value decrypted

5 It is to be noted that it is not necessary for the policy agent to have received the data packets from the user when it constructs the challenge. The policy agent, however, can calculate the second digest value (step 122, Fig. 4) only after having received the data packets. If the policy agent
10 receives the data packets from the client computer prior to calculating the challenge or before the user is authenticated, it should buffer the data and not forward them to their destination until the authentication process has been completed.

25 By way of example, the construction of the challenge and
response in a preferred embodiment is described below.
Referring now to FIG. 5, in this embodiment, the underlying

25 By way of example, the construction of the challenge and
response in a preferred embodiment is described below.
Referring now to FIG. 5, in this embodiment, the underlying

protocol for the transmission of network data is the widely used TCP/IP. Each of the client computer and the policy agent is identified by an IP address, and the network connection between them is further identified by a port number of the client computer and a port number of the policy agent. The network data sent by the user at the client computer are transmitted in the form of communication packets 96 (FIG. 3). When the policy agent 78 detects the network connection from client computer 72, it obtains the name of the unauthenticated user who purportedly used the client computer to initiate the connection. The policy agent then proceeds to look up the public key PUBKu of the user of the client computer. The policy agent knows its own public key PUBKp and private key PRVKp. In addition to the user's public key PUBKu, the policy agent obtains the following information from the operating system:

IPc - the IP address of the client computer;
PORTc - the IP connection port of the client computer;
PORTp - the IP connection port of the policy agent;
T - the system time;
RND1 - a random number.

The policy agent then constructs a challenge for user authentication based on these five values. As illustrated in FIG. 5, these five values are concatenated, and the resultant value 136 is used as the input of a hash function 138 to generate a hash value H1. The hash function 138 may be, for

example, the MD5 algorithm known to those skilled in the art.

This step of generating the hash value is represented by the following expression:

$$H1 = MD5(RND1*PORTp*PORTc*IPc*T),$$

5 where the symbol "*" means concatenation. The hash value H1 is then encrypted first with the private key PRVKp of the policy agent and then with the public key PUBKu of the purported user to form the challenge 90. This step is represented by the following expression:

$$10 \quad C = PUBKu(PRVKp(H1)),$$

wherein C is the challenge. The challenge 90 is sent by the policy agent 78 to the client computer 72.

As shown in FIG. 6, when the client computer 72 that initiated the connection receives the challenge 90, it
 15 decrypts the challenge 90 using the user's private key PRVKu and the policy agent's public key PUBKp. If the public key PUBKu used to encrypt the challenge 90 indeed belongs to the user, the client computer would be able to decrypt the challenge to obtain the hash number H1. The client computer
 20 then constructs a response 94 that ties the user authentication to the network data stream. To prepare the response 94, the client computer concatenates a random number RND2, the decrypted hash H1, and data DATAnp from the first N packets of the transmitted network data, where N is a pre-
 25 selected number, such as five (5). The concatenated value 150 is then used as the input for a hash function 152, such as the

MD5 algorithm, to generate a second hash value H2. This step is represented by the following expression:

$$H2 = MD5(RND2 * H1 * DATA_{np}).$$

The hash value H2 is then concatenated with the random number RDN2, and the concatenated value 154 is encrypted first with the user's private key PRVKu and then with the public key PUBKp of the policy agent to form the response 94. This step is represented by the following expression:

$$R = PUBKp(PRVKu(H2 * RND2)),$$

where R is the response. The response 94 is then sent to the policy agent 78.

Turning now to FIG. 7, when the policy agent 78 receives the response 94 from the client computer, it decrypts the response using its own private key PRVKp and the public key PUBKu of the user to obtain the hash H2 and the random number RDN2. To verify that the hash number H2 from the decrypted response is what it should be, the policy agent calculates a hash value H2p using the hash value H1 included in the challenge 90, the random number RND2 from the decrypted response 94, and the data RDATA_{np} of the first N packets of the received network data as the input for the hash function.

An agreement between the hash value H2p calculated by the policy agent and the hash value H2 decrypted from the response 94 indicates that the user is who she claims to be, and that the network data received by the policy agent from the client computer are indeed those sent by the user. In other words, the validation of the response serves two functions:

authenticating the user and associating the received network with the authenticated user. The user is authenticated because only the real user would have the private key to properly decrypt the challenge and construct a valid response.

- 5 The network data are confirmed to be those sent by the user because if the data packets received by the policy agent have been maliciously altered, the hash value H2p calculated by the policy agent would be different from the hash value H2 obtained from the response. In addition to the user
- 10 authentication and data stream association, the hash value H2 can now be used as a one-time shared secret for further session encryption.

- In the embodiment described above, the public keys PUBKp and PUBKu of the policy agent and the user, respectively, are
- 15 used for encryption in the challenge-response process. In another embodiment, to speed up the process, the policy agent can opt not encrypt the challenge with the public key PUBKu of the user, and the client computer will also not encrypt the response with the public key PUBKp of the policy agent. This
- 20 process saves two public-key encryption steps and the corresponding private-key decryption steps. In this case, however, the hash value H2 may be obtained by a malicious attacker by intercepting the response and decrypting it with the public key PUBKu of the user. As a result, the hash H2 is
- 25 preferably not used as a shared secret for further encryption.

In view of the foregoing, it can be seen that the present invention provides an effective method and system for a policy

agent to authenticate a user that sends a network data stream. The authentication process is performed out-of-band and is thus independent of the protocols used to transmit the network data. The authentication process according to the invention
5 not only verifies the identity of the user sending the network packets but also associates the network data stream received by the policy agent with the user being authenticated.

In view of the many possible embodiments to which the principles of this invention may be applied, it should be
10 recognized that the embodiment described herein with respect to the drawing figures is meant to be illustrative only and should not be taken as limiting the scope of invention. For example, those of skill in the art will recognize that the elements of the illustrated embodiment shown in software may
15 be implemented in hardware and vice versa or that the illustrated embodiment can be modified in arrangement and detail without departing from the spirit of the invention. Therefore, the invention as described herein contemplates all such embodiments as may come within the scope of the following
20 claims and equivalents thereof.

5507-575450

What is claimed is:

1. A computer-readable medium having computer-executable
5 instructions for operating a policy agent of a network for
performing steps comprising:

detecting a network connection from a client computer on
the network;

composing a challenge for authenticating a user of the
10 client computer associated with said network connection, the
challenge being encrypted with a private key of the policy
agent;

transmitting the challenge to the client computer;

receiving a response from the client computer;

15 decrypting the response using a public key of the user to
obtain a first message digest value;

receiving network data through the network connection
with the client computer;

calculating a second message digest value based on the
20 challenge and the received network data;

comparing the first and second message digest values to
determine whether a match is found.

2. A computer-readable medium as in claim 1, wherein the
25 policy agent is a firewall.

65607-52460

3. A computer-readable medium as in claim 1, wherein the step of composing including encrypting the challenge with a public key of the user.

5 4. A computer-readable medium as in claim 3, wherein the step of decrypting includes decrypting the response with a private key of the policy agent.

10 5. A computer-readable medium as in claim 1, wherein the step of composing includes generating a third digest value from data including a time value, and encrypting the third digest value with the private key of the policy agent.

15 6. A computer-readable medium as in claim 1, wherein the received network data are in a form of packets, and the step of calculating calculates the second message digest value based on a pre-selected number of packets of the received network data.

20 7. A computer-readable medium as in claim 1, having further computer-executable instructions for performing network access policies on the received network data according to the identity of the user after a match between the first and second message digest values is found.

8. A method of authenticating a user using a client computer on a network to transmit network data through a policy agent of the network, comprising the steps of:

detecting by the policy agent a network connection from
5 the client computer for transmitting network data of the user;

receiving by the policy agent network data transmitted through the network connection from the client computer;

obtaining, by the policy agent, identity of the user and a public key of the user;

10 composing, by the policy agent, a challenge encrypted with a private key of the policy agent;

sending the challenge to the client computer;

decrypting, by the client computer, the challenge;

generating, by the client computer, a first message
15 digest value based on the challenge and the network data of the user;

encrypting, by the client computer, the first message digest value with a private key of the user to create a response;

20 sending the response to the policy agent;

decrypting, by the policy agent, the response to obtain the first message digest value;

calculating, by the policy agent, a second message digest value based on the challenge and the network data received
25 through the network connection from the client computer;

comparing the first and second message digest values to determine whether there is a match therebetween.

56075340

9. A method as in claim 8, further including the step of applying network policies by the policy agent on the received network data based on the identity of the user after a match between the first and second message digest values is found.

5

10. A method as in claim 8, wherein the step of composing the challenge includes encrypting the challenge with the public key of the user.

10

11. A method as in claim 8, wherein the step of encrypting by the client computer includes encrypting the first message digest value with a public key of the policy agent.

15

12. A method as in claim 8, wherein the step of composing the challenge includes generating a third message digest value based on data including a time value and encrypting the third message digest value to form the challenge.

20

13. A method as in claim 8, wherein the received network data are in a form of packets, and the step of generating by the client computer generates the first message digest value based on data of a pre-selected number of packets of the received network data.

25

665077-6E9E460

14. A method as in claim 8, wherein the step of
generating by the client computer generates the first message
digest value based on a random number, data decrypted from the
challenge, and data of the pre-selected packets of the
5 received network data.

15. A method as in claim 8, wherein the policy agent is
a firewall of the network.

ABSTRACT

A policy agent of a network performs an out-of-band user authentication process to verify the identity of a user of a client computer and associates the network data received from the client compute with the user. When the client computer initiates a network data connection to or through the policy agent, the policy agent sends an encrypted challenge to the client computer. The challenge is encrypted with a private key of the policy agent. When the client computer received the challenge, it decrypts the challenge and prepares a message digest value based on the challenge and the network data sent by the user. The message digest value is then encrypted with the private key of the user to form a response, and the response is sent to the policy agent. The policy agent decrypts the response with the public key of the user to obtain the message digest value and calculates a digest value based on the challenge and the received network data. The policy agent then compares the calculated digest value with the decrypted digest value. A match between the two digest values indicates that the user is successfully authenticated, and that the received network data is associated with the user. The policy agent may then apply network policies based on the credentials of the authenticated user.

5507 334450

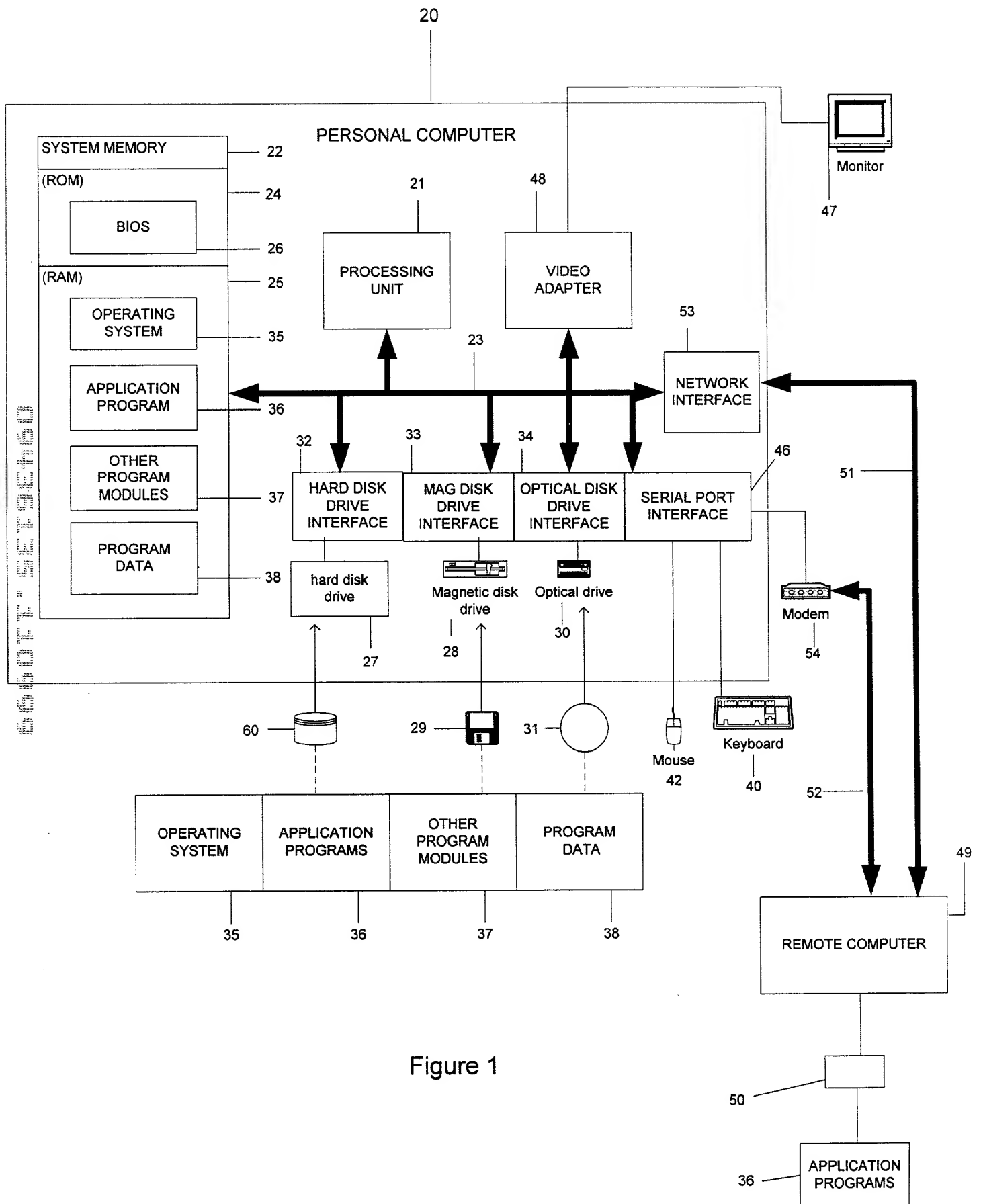


Figure 1

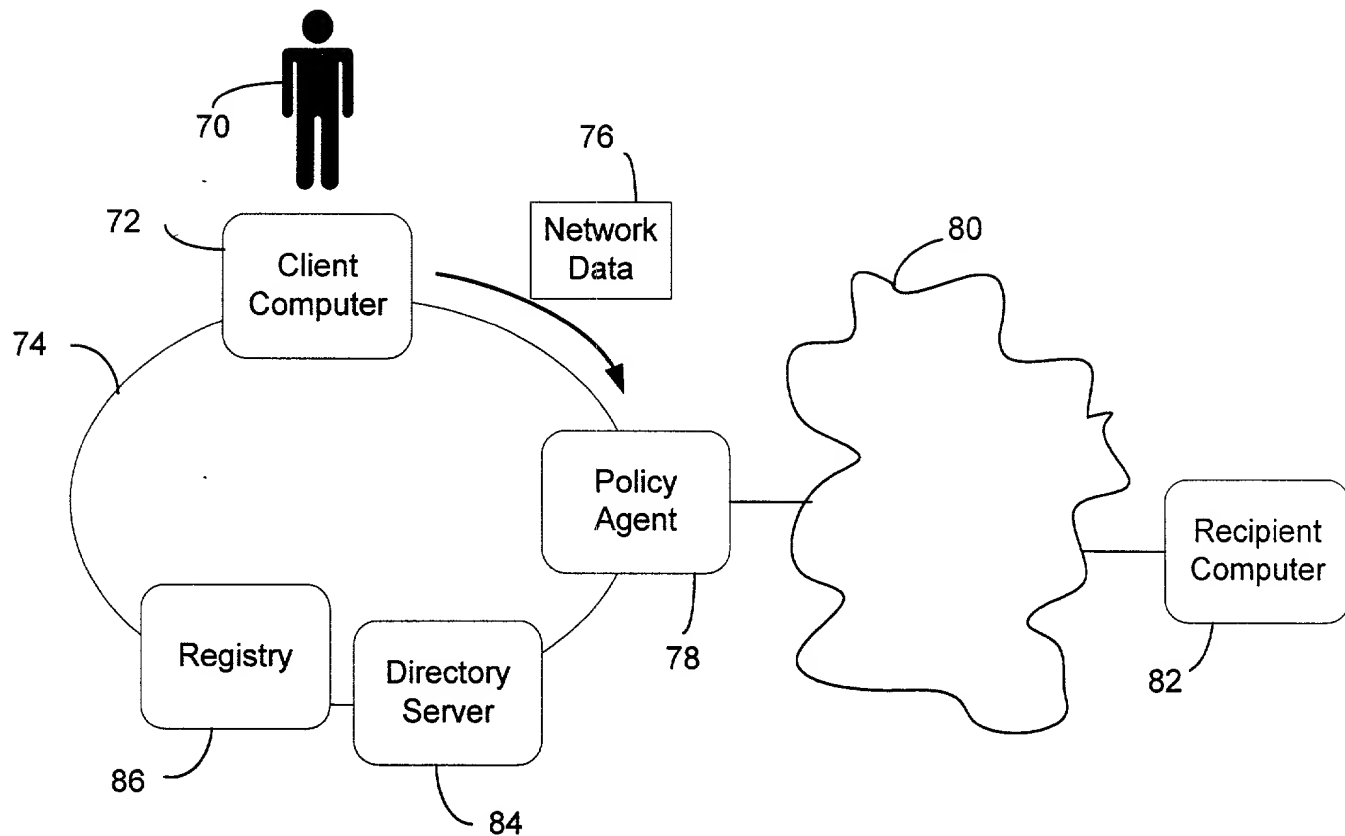


FIG. 2

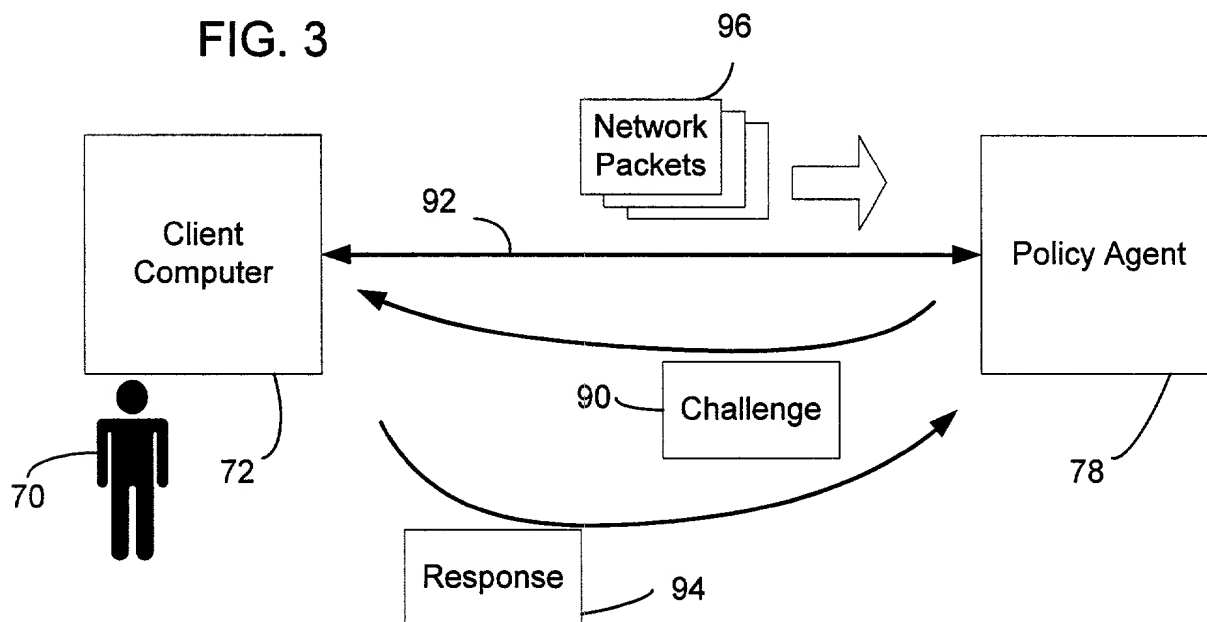


FIG. 3

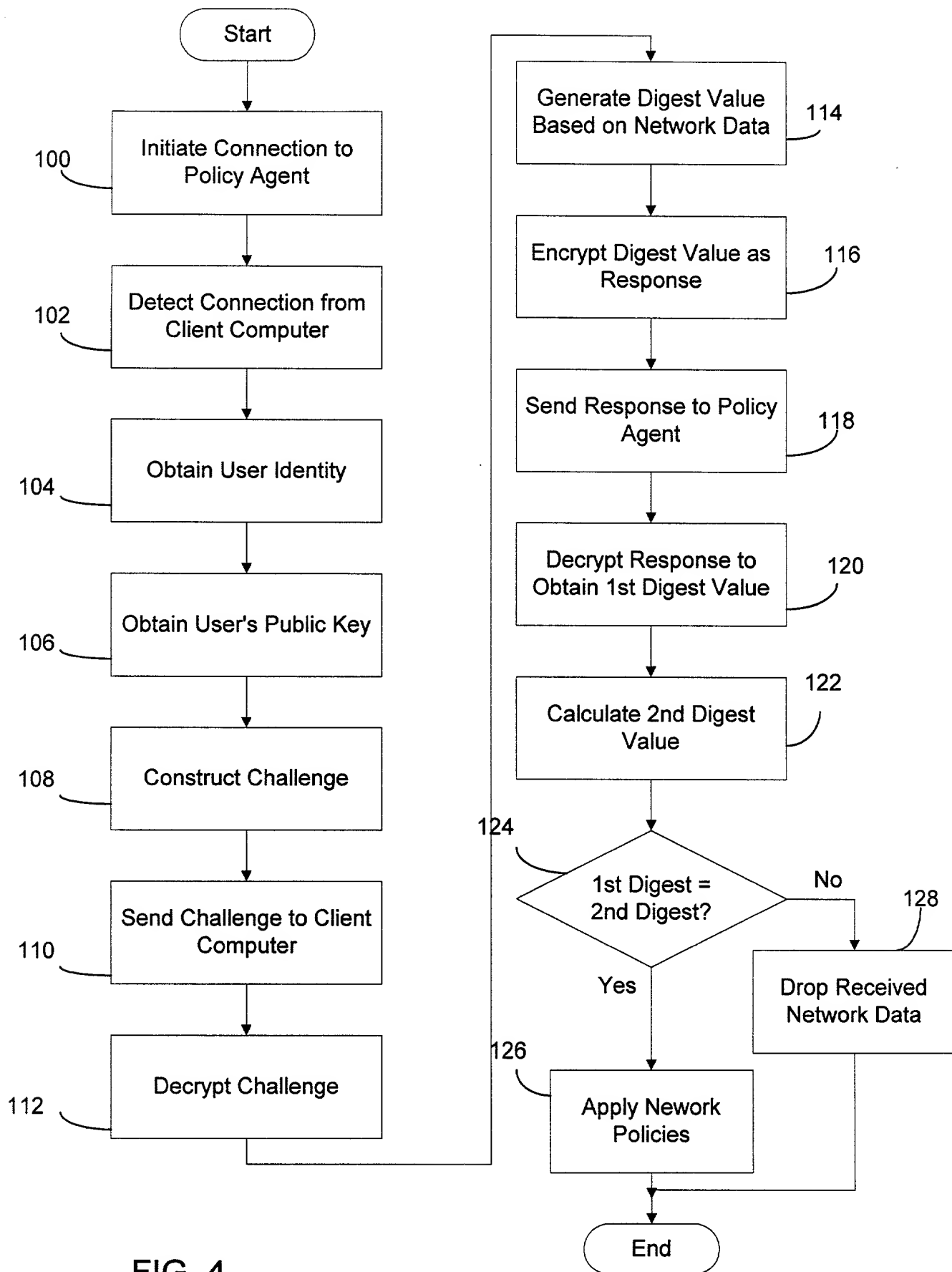


FIG. 4

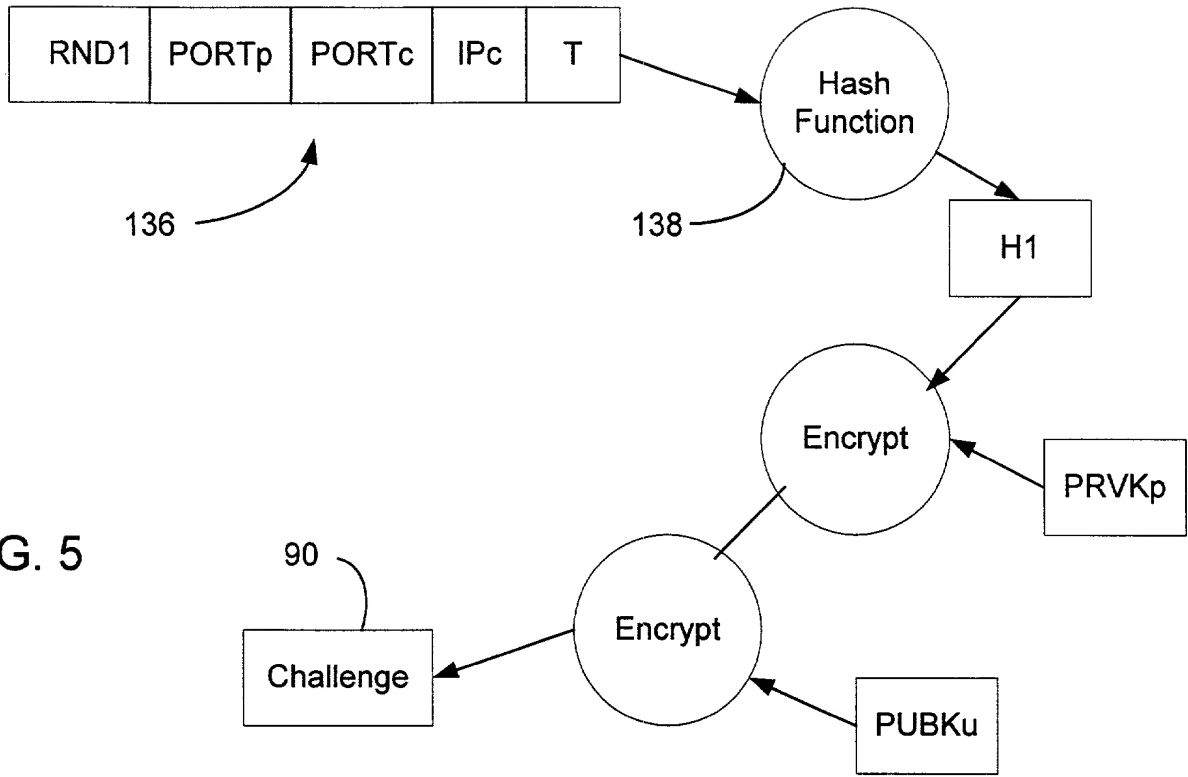


FIG. 5

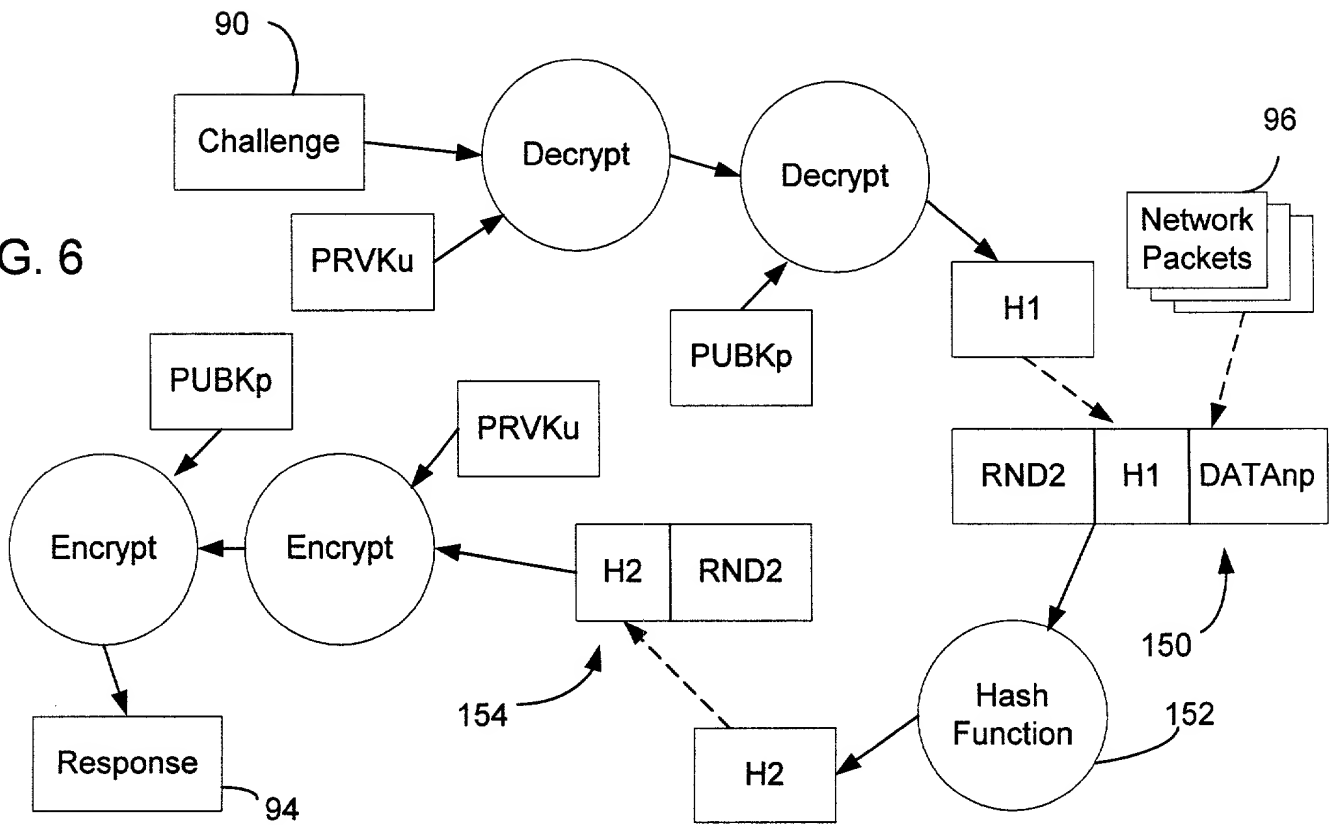


FIG. 6

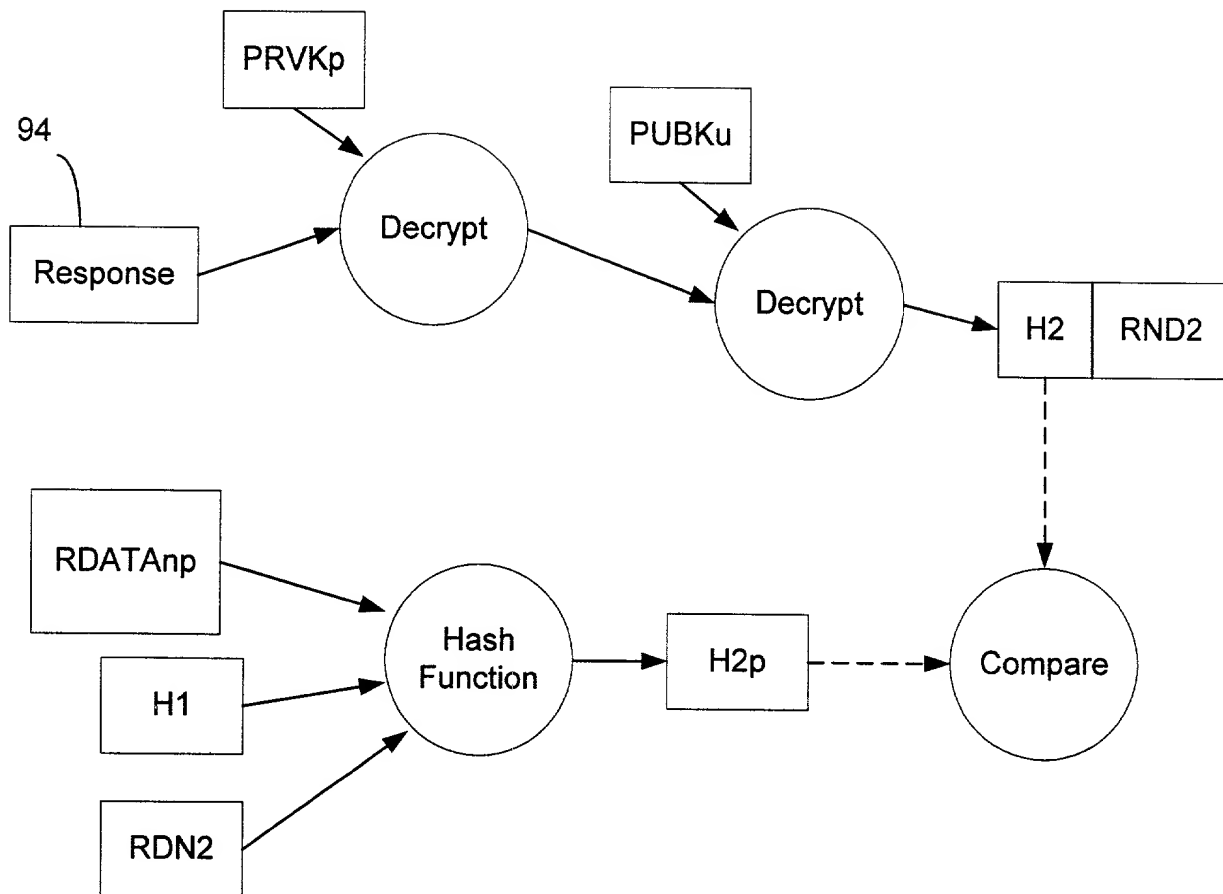


FIG. 7

COMBINED DECLARATION AND POWER OF ATTORNEY

As below named inventor, I hereby declare that

This declaration is of the following type:

- ☒ original ☐ design ☐ supplemental
☐ national stage of PCT
☐ divisional ☐ continuation ☐ continuation-in-part

My residence, post office address, and citizenship are as stated below next to my name. I believe I am the original, first, and sole inventor (*if only one name is listed below*) or an original, first, and joint inventor (*if plural names are listed below*) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD OF USER AUTHENTICATION FOR NETWORK
COMMUNICATION THROUGH A POLICY AGENT

the specification of which:

- ☒ is attached hereto.
☐ was filed on _____ as Serial No. _____ and was amended on _____. (*if applicable*).
☐ was filed by Express Mail No. _____ as Serial No. not known yet, and was amended on _____ (*if applicable*).
☐ was described and claimed in PCT International Application No. _____ filed on _____ and as amended under PCT Article 19 on _____ (*if any*).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

COUNTRY	APPLICATION	DATE OF FILING (day,month,year)	PRIORITY CLAIMED UNDER 35 USC 119		
				YES	NO
				YES	NO
				YES	NO
				YES	NO

In re Application of Gunter et al.
U.S. Patent Application, Serial No. Not Yet Assigned

I hereby claim the benefit pursuant to Title 35, United States Code, § 119(e) of the following United States provisional application(s):

PRIOR U.S. PROVISIONAL APPLICATIONS CLAIMING THE BENEFIT UNDER 35 USC 119(e)	
APPLICATION NO.	DATE OF FILING

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application.

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 USC 120					
U.S. APPLICATIONS			Status (<i>check one</i>)		
U.S. APPLICATIONS	U.S. FILING DATE		PATENTED	PENDING	ABANDONED
1. 0 /					
2. 0 /					
3. 0 /					
PCT APPLICATIONS DESIGNATING THE U.S.			Status (<i>check one</i>)		
PCT APPLICATION NO.	PCT FILING DATE	U.S. SERIAL NOS. ASSIGNED (if any)	PATENTED	PENDING	ABANDONED
4.					
5.					
6.					

DETAILS OF FOREIGN APPLICATIONS FROM WHICH PRIORITY CLAIMED UNDER 35 USC 119 FOR ABOVE LISTED U.S./PCT APPLICATIONS				
ABOVE APPLN. NO.	COUNTRY	APPLICATION NO.	DATE OF FILING (day,month,yr)	DATE OF ISSUE (day,month,yr)
1.				
2.				
3.				
4.				

In re Application of Gunter et al.
U.S. Patent Application, Serial No. Not Yet Assigned

As a named inventor, I hereby appoint the following attorneys to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Berton Scott Sheppard, Reg. 20922
James B. Muskal, Reg. 22797
Dennis R. Schlemmer, Reg. 24703
Gordon R. Coons, Reg. 20821
John E. Rosenquist, Reg. 26356
John W. Kozak, Reg. 25117
Charles S. Oslakovic, Reg. 27583
Mark E. Phelps, Reg. 28461
H. Michael Hartmann, Reg. 28423
Bruce M. Gagala, Reg. 28844
Charles H. Mottier, Reg. 30874
John Kilyk, Jr., Reg. 30763
Robert F. Green, Reg. 27555
John B. Conklin, Reg. 30369
James D. Zalewa, Reg. 27848
John M. Belz, Reg. 30359
Brett A. Hesterberg, Reg. 31837
Jeffrey A. Wyand, Reg. 29458

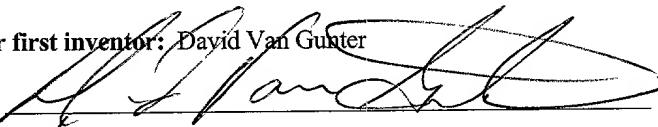
Paul J. Korniczky, Reg. 32849
Pamela J. Ruschau, Reg. 34242
Steven P. Petersen, 32927
John M. Augustyn, Reg. 33589
Christopher T. Griffith, Reg. 33392
Wesley O. Mueller, Reg. 33976
Jeremy M. Jay, Reg. 33587
Jeffrey B. Burgan, Reg. 35463
Eley O. Thompson, Reg. 36035
Mark Joy, Reg. 35562
Allen E. Hoover, Reg. 37354
David M. Airan, Reg. 38811
Michael H. Tobias, Reg. 32948
Xavier Pillai, Reg. 39799
Y. Kurt Chang, Reg. 41397
Gregory C. Bays, Reg. 40505
Carol Larcher, Reg. 35243

Steven H. Sklar, Reg. 42154
M. Daniel Hefner, Reg. 41826
Thomas A. Belush, Reg. 37090
Kenneth P. Spina, Reg. 43927
Gary R. Jarosik, Reg. 35906
Song Zhu, Reg. 44420
Jeffery J. Makeever, Reg. 37390
Salim A. Hasan, Reg. 38175
Richard A. Wulff, Reg. 42238
Jamison E. Lynch, Reg. 41168
Rattan Nath, Reg. 43827
Robert M. Gould, Reg. 43642
Kevin L. Wingate, Reg. 38662
David J. Schodin, Reg. 41294
Paul L. Ahern, Reg. 17020
Theodore W. Anderson, Reg. 17035
Noel I. Smith, Reg. 18698
Katie E. Sako, Reg. 32628
Daniel D. Crouse, Reg. 32022

I further direct that correspondence concerning this application be directed to LEYDIG, VOIT & MAYER, LTD., Two Prudential Plaza, Suite 4900, 180 North Stetson, Chicago, Illinois 60601-6780, Telephone (312) 616-5600.

I hereby declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: David Van Gunter

Inventor's signature 

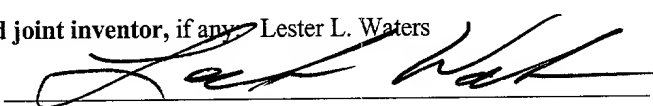
Date 10/25/99

Country of Citizenship: US

Residence: 17511 NE 22nd Court, Redmond, Washington 98052

Post Office Address: Same as above

Full name of second joint inventor, if any: Lester L. Waters

Inventor's signature 

Date Nov. 8, 1999

Country of Citizenship: US

Residence: 954 Broadway Avenue E, Unit 101, Seattle, Washington 98101

Post Office Address: Same as above